

Załącznik nr 1 WIF-RZPO.272.00027.2024

Szczegółowy opis przedmiotu zamówienia

1. Informacje ogólne

Niniejsza specyfikacja określa wymagania funkcjonalne i techniczne w zakresie dostawy oprogramowania antywirusowego dla Starostwa Powiatowego w Gliwicach.

Siedziba Zamawiającego: Starostwo Powiatowe w Gliwicach,

ul. Zygmunta Starego 17,

44-100 Gliwice

2. Przedmiotem zamówienia jest:

- 1) dostawa wraz z wdrożeniem licencji oprogramowania antywirusowego w wersji ESET PROTECT ADVANCED lub równoważnego, spełniającego wymagania określone w niniejszej OPZ,
- 2) przeprowadzenie szkolenia (instruktaż).

Zamawiający wskazuje, że realizacja przedmiotu zamówienia może nastąpić poprzez zaoferowanie nowej licencji pakietu antywirusowego lub poprzez upgrade posiadanej przez Zamawiającego licencji w wersji ESET PROTECT ESSENTIAL, w liczbie wskazanej w Tabeli nr 1.

Przedmiot zamówienia jest realizowany w ramach projektu „Cyberbezpieczny Powiat Gliwicki”, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, Priorytetu II Zaawansowane usługi cyfrowe programu Fundusze Europejskie na Rozwój Cyfrowy (FERC) dofinansowanego z Unii Europejskiej, z Europejskiego Funduszu Rozwoju Regionalnego (EFRR).

3. Wykaz dostaw, instalacji i konfiguracji

Mając na uwadze charakter postępowania Zamawiający w tabeli nr 5.1 przyporządkował cechy oprogramowania i szkolenia będących przedmiotem niniejszego postępowania, które szczegółowo opisane zostały w dalszej części niniejszego załącznika do SWZ. Dodatkowo w poniższej tabeli nr 1 zawarto informacje na temat liczby licencji jakie Wykonawca będzie zobligowany dostarczyć po podpisaniu umowy, której wzór jest integralną częścią SWZ.

Plan wdrożenia:

- 1) Wykonawca przygotuje i omówi koncepcję konfiguracji z administratorem sieci Zamawiającego.
- 2) Wykonawca będzie uzgadniał z Zamawiającym harmonogram instalacji.
- 3) Wdrożenia nowego oprogramowania musi uwzględniać aspekt współpracy/integracji z innymi systemami i urządzeniami (typu przełączniki, Active Directory) będących w posiadaniu Zamawiającego. Dodatkowo każda zmiana w koncepcji musi być każdorazowo uzgadniana z administratorem sieci.

- 4) Wykonawca omówi z Zamawiającym stan końcowy konfiguracji i w porozumieniu z Zamawiającym dopracuje szczegółowość konfiguracji.
- 5) Przeprowadzenie instruktażu stanowiskowego z konfiguracji oraz „dobrych praktyk” w zakresie stosowanej technologii (1 dzień dla 4 administratorów min. 4 godzin łącznie), zakończone certyfikatem lub zaświadczeniem odbycia szkolenia.
- 6) Przekazanie dokumentacji powdrożeniowej.

Tabela 1. Przyporządkowanie cech technicznych

lp	Urządzenie/Usługa	Liczba sztuk	Cecha
1	2	3	4
1	ESET PROTECT ADVANCED	500	A

4. Wymagania co do gwarancji i obsługi serwisowej

Szczegółowy zakres gwarancji został ujęty w pkt. 5 Szczegółowego Opisu Przedmiotu Zamówienia i w Umowie.

Zamawiający dopuszcza zastosowanie programów równoważnych innych niż określone w SWZ. Ciężar udowodnienia, że oferowane oprogramowanie jest równoważne w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy.

Wszystkie wskazane z nazwy programy i funkcje występujące w szczegółowym opisie przedmiotu zamówienia należy rozumieć jako określenie wymaganych minimalnych parametrów technicznych lub standardów jakościowych. Oznacza to, że zgodnie z art. 99 oraz 101 ustawy Prawo zamówień publicznych wskazaniom tym towarzyszą wyrazy „lub równoważne”. Wykonawca, który w ofercie powoła się na zastosowanie rozwiązań urządzeń równoważnych opisanych w SWZ, jest obowiązany wykazać, że oferowane oprogramowanie urządzenia spełnia wymagania określone przez Zamawiającego.

5. Minimalne wymagania stawiane dla oprogramowania i usług świadczonych w ramach niniejszego postępowania

1) Oprogramowanie antywirusowe - Cecha A

L.P.	Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
1	2	3
1	Gwarancja, serwis, licencje	- Licencja musi korzystać z aktualnych baz silnika detekcji ochronnych producenta oprogramowania w zakresie Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android) na okres do 6 marca 2026 roku. - Licencja musi być objęty serwisem gwarancyjnym producenta przez okres do 6 marca 2026 roku. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. - Do zamawianego oprogramowania Wykonawca zapewni usługi wsparcia technicznego w języku polskim w zakresie: - obsługa procesu RMA u producenta, - zdalna pomoc w skonfigurowaniu oprogramowania do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta, - pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu, - doradztwo w zakresie konfiguracji, - zdalne wsparcie techniczne, - pomoc w zakładaniu zgłoszeń serwisowych u producenta. - Dostęp do usługi powinien być świadczony przez dedykowane numery telefonu oraz przez dedykowany moduł internetowy (w umowie należy podać adres oraz numery telefonów).
2	Administracja zdalna w chmurze	- Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. - Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. - Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. - Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. - Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. - Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. - Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. - Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. - Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. - Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. - Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. - Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, co tygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

3	Ochrona stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, a. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, b. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, c. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, d. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
---	--------------------------	--

		17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne). 21. Rozwiązanie musi posiadać funkcjonalność skanera EFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 24. Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki. 25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
--	--	---

4	Ochrona serwera	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
5	Dodatkowe wymagania dla ochrony serwerów Windows	1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 6. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
6	Dodatkowe wymagania dla ochrony serwerów Linux	1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.

7	Szyfrowanie	1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8	Ochrona urządzeń mobilnych opartych o system Android	1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenia do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła

9	Sandbox w chmurze	1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: a. Czysty, b. Podejrzany, c. Bardzo podejrzany, d. Szkodliwy. 13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.
---	-------------------	--

Opracował:

Łukasz Szyszko

(imię i nazwisko)

(podpis)